



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/749,412	01/02/2004	Ryo Ochi	247305US6	2841
22850	7590	08/15/2007		
OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C. 1940 DUKE STREET ALEXANDRIA, VA 22314			EXAMINER LE, CANH	
			ART UNIT 2139	PAPER NUMBER
			NOTIFICATION DATE 08/15/2007	DELIVERY MODE ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary

Application No.

10/749,412

Applicant(s)

OCHI ET AL.

Examiner

Canh Le

Art Unit

2139

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 02 January 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-22 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-22 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 02 January 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

This Office Action is in response to the application filed on 01/02/2004. Claims 1-22 are pending and have been examined.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 21-22 are rejected under 35 U.S.C. 101 because the claimed invention are directed to non-statutory subject matter.

Claims 21 and 22 are ejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Computer programs written to perform encryption processing on a computer system are not physical "things". They are neither computer components nor statutory process, as they are not "acts" being performed. The computer program does not define any structural and functional interrelationships between the computer program and other claimed elements of a computer which permit the computer program's functionality to be realized.

Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Art Unit: 2139

Claims 1-2, 11-12, and 21 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1, 11, and 21 recite the limitation "the condition " in lines 9-10. There are insufficient antecedent bases for this limitation in the claims.

Claims 2 and 12 recite the limitation "a dummy encryption processing" in lines 2-3 where its meaning is unclear. This ambiguity renders claims 2 and 12 indefinite.

The Examiner interprets "a dummy encryption processing" which does not do any encryption processing.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 3-5, 8, 11, 13-15, 18, and 21 are rejected under 35 U.S.C. 102(b) as being anticipated by **Henry Kuo et al.**, "Architectural Optimization for a 1.82 Gbits/sec VLSI Implementation of the AES Rijndael Algorithm", Springer-Verlag Berlin, LNCS 2162, pp. 51-64, 2001.

As per claims 11, 1, 21:

Claim 11

Kuo teaches an encryption processing method for performing a data encryption process, said encryption processing method comprising:

(a) a division step of dividing an original encryption processing sequence into a plurality of groups composed of one or more encryption processing units **[pg. 56, section 3.5.1 Substitution, fig. 4; “The 256 bit data is broken down into 32 chunks, 8 bit each, and each of them is used as the address for S-box table lookup ... the block diagram for this module”];**

(b) a mixed encryption processing sequence setting step of setting a mixed encryption processing sequence by mixing processing sequences of encryption processing units under the condition in which the processing sequence of the encryption processing units, set in said division step, within each group is fixed **[pg. 57, section 3.5.3 Mix Column, fig. 6; “In Mix Column, four bytes in the corresponding position in the four “rows” are used for matrix multiplication in $GF(2^8)$, which involves byte-wise multiplication and addition ... generating the first byte of each row”];** and

(c) an encryption processing step of performing an encryption process in accordance with the mixed encryption processing sequence set in said mixed encryption processing sequence setting step **[pg. 57, section 3.5.3 Mix Column, fig. 6; “In Mix Column, four bytes in the corresponding position in the four “rows” are used for matrix multiplication in $GF(2^8)$, which involves byte-wise multiplication**

Art Unit: 2139

and addition ... generating the first byte of each row”].

Claims 1 and 21 are essentially the same as claim 11 except that they set forth the claimed invention as an apparatus / a computer program rather than a method and rejected under the same reasons as applied above.

As per claims 13, 3:

Claim 13

Kuo teaches An encryption processing method according to claim 11, wherein said division step determines a group of sequences, which can be performed independently of each other, within the original encryption processing sequence to be divided in a process of division into a plurality of groups composed of one or more encryption processing units, and performs a process for setting a group of divisions in which the sequence which can be performed independently is a unit [pg. 56, section 3.5.1 Substitution, fig. 4; “The 256 bit data is broken down into 32 chunks, 8 bit each, and each of them is used as the address for S-box table lookup ... the block diagram for this module”; each S-box is an encryption processing and performs independently as a unit].

Claim 3 is essentially the same as claim 13 except that they set forth the claimed invention as an apparatus rather than a method and rejected under the same reasons as applied above.

As per claims 14, 4:

Claim 14

Kuo teaches an encryption processing method according to claim 11, wherein said encryption processing unit is a single-DES encryption process, said division step divides the original encryption processing sequence containing one or more single-DES encryption processes into a plurality of groups composed of one or more single-DES encryption processes, and said mixed encryption processing sequence setting step sets one mixed encryption processing sequence by mixing the single-DES encryption processing units contained in each group of divisions by mutual replacement of the single-DES encryption processing units of each set group under the condition in which the processing sequence within each set group is fixed [pg. 56, section 3.5.1

Substitution, fig. 4; “The 256 bit data is broken down into 32 chunks, 8 bit each, and each of them is used as the address for S-box table lookup ... the block diagram for this module”; pg. 51; “The AES Rijndael algorithm was chosen in October 2000 and is expected to replace the DES and Triple DES”. A single-DES includes S-box substitution].

Claim 4 is essentially the same as claim 14 except that they set forth the claimed invention as an apparatus rather than a method and rejected under the same reasons as applied above.

Art Unit: 2139

As per claims 15, 5:**Claim 15**

Kuo teaches an encryption processing method according to claim 11, wherein the original encryption processing sequence to be mixed is an encryption processing sequence including a triple-DES encryption process, and said division step performs a process for dividing the encryption processing sequence into a plurality of groups composed of one or more encryption processing units with the single-DES encryption process which forms the triple-DES encryption process being an encryption processing unit [pg. 56, section 3.5.1 Substitution, fig. 4; “The 256 bit data is broken down into 32 chunks, 8 bit each, and each of them is used as the address for S-box table lookup ... the block diagram for this module”; pg. 57, section 3.5.3 Mix Column, fig. 6; pg. 51; “The AES Rijndael algorithm was chosen in October 2000 and is expected to replace the DES and Triple-DES”. The Triple-DES includes three single DES].

Claim 5 is essentially the same as claim 15 except that they set forth the claimed invention as an apparatus rather than a method and rejected under the same reasons as applied above.

As per claims 18, 8:

Claim 18

Kuo teaches an encryption processing method according to claim 11, wherein said encryption processing step includes a step of storing processing results in a memory for storing processing results of the encryption processing units which form the mixed encryption processing sequence in such a manner as to be capable of identifying which encryption processing unit the processing results are obtained from [pg. 55, **section 3.3 Memory Architecture Optimization; "The design is based on one clock cycle for each encryption round, we have to duplicate memory several times"**].

Claim 8 is essentially the same as claim 18 except that they set forth the claimed invention as an apparatus rather than a method and rejected under the same reasons as applied above.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 2, 7, 9, 10, 12, 17, 19-20, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Henry Kuo et al.**, "Architectural Optimization for a 1.82 Gbits/sec

VLSI Implementation of the AES Rijndael Algorithm”, Springer-Verlag Berlin, LNCS 2162, pp. 51-64, 2001 in view of **Bo Lin et al.** (GB 2 345 229 A).

As per claims 12 and 2:

Claim 12

Kuo does not teach, “an encryption processing method comprising the step of setting a dummy encryption processing unit ...mixing the encryption processing units of a plurality of groups containing said dummy encryption processing units”.

However, Lin teaches an encryption processing method comprising the step of setting a dummy encryption processing unit for performing a dummy encryption process unnecessary for said original encryption processing sequence in at least one of said groups of divisions, and said mixed encryption processing sequence setting step sets one mixed encryption processing sequence by mixing the encryption processing units of a plurality of groups containing said dummy encryption processing units [**abstract, pg. 11, lines 10-28**”; **“Another technique which could be used to improve resistance to attacks is to insert “dummy” operation to confuse analysis of a power signature... The number of dummy look-ups performed can be chosen to optimize the time it takes to perform the DES operation and the benefit gained in DPA attack resistance”**].

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the encryption processing method of Kuo of the

invention by including the step of Lin because it would perform the DES operation and the benefit gained in DPA attack resistance **[Lin, pg. 11, lines 18-19]**.

Claim 2 is essentially the same as claim 12 except that they set forth the claimed invention as an apparatus rather than a method and rejected under the same reasons as applied above.

As per claims 17, 7:

Claim 17

Kuo teaches An encryption processing method according to claim 11, wherein the original encryption processing sequence to be mixed is an encryption processing sequence including a triple-DES encryption process, said division step divides the encryption processing sequence into a plurality of groups composed of one or more encryption processing units by using the single-DES encryption process which forms the triple-DES encryption process as an encryption processing unit **[pg. 56, section 3.5.1 Substitution, fig. 4; “The 256 bit data is broken down into 32 chunks, 8 bit each, and each of them is used as the address for S-box table lookup ... the block diagram for this module”; pg. 51; “The AES Rijndael algorithm was chosen in October 2000 and is expected to replace the DES and Triple DES”. A single-DES includes S-box substitution]**.

Kuo does not teach a process for setting a dummy single-DES process as a dummy encryption process unnecessary for the original encryption processing

sequence in at least one of said groups of divisions, and for setting the number of single-DES processes of dummies to be set to a multiple of 3 corresponding to the triple DES.

However, Lin teaches setting a dummy single-DES process as a dummy encryption process unnecessary for the original encryption processing sequence in at least one of said groups of divisions, and for setting the number of single-DES processes of dummies to be set to a multiple of 3 corresponding to the triple DES **[abstract, pg. 11, lines 10-28”;** “Another technique which could be used to improve resistance to attacks is to insert “dummy” operation to confuse analysis of a power signature... The number of dummy look-ups performed can be chosen to optimize the time it takes to perform the DES operation and the benefit gained in DPA attack resistance”. It is obvious for setting the number of single-DES processes of dummies to be set to a multiple of 3 corresponding to the triple DES because each number of single-DES is set to 1].

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the encryption processing method of Kuo of the invention by including the step of Lin because it would perform the DES operation and the benefit gained in DPA attack resistance **[Lin, pg. 11, lines 18-19].**

Claim 7 is essentially the same as claim 17 except that they set forth the claimed invention as an apparatus rather than a method and rejected under the same reasons as applied above.

As per claim 19, 9, 22:

Claim 19

Kuo teaches an encryption processing method for performing a data encryption process, said encryption processing method comprising:

(a) a division step of dividing an original encryption processing sequence into one or more encryption processing units [pg. 56, section 3.5.1 Substitution, fig. 4; “The 256 bit data is broken down into 32 chunks, 8 bit each, and each of them is used as the address for S-box table lookup ... the block diagram for this module”];

(b) a mixed encryption processing sequence setting step of setting a mixed encryption processing sequence [pg. 57, section 3.5.3 Mix Column, fig. 6; “In Mix Column, four bytes in the corresponding position in the four “rows” are used for matrix multiplication in GF (2^8), which involves byte-wise multiplication and addition ... generating the first byte of each row”].

(c) an encryption processing step of performing an encryption process in accordance with said mixed encryption processing sequence [pg. 57, section 3.5.3 Mix Column, fig. 6; “In Mix Column, four bytes in the corresponding position in the four “rows” are used for matrix multiplication in GF (2^8), which involves byte-wise multiplication and addition ... generating the first byte of each row”].

Kuo does not teach, “adding a dummy encryption processing unit for performing a process ... dummy encryption processing units”.

However, Lin teaches adding a dummy encryption processing unit for performing a process corresponding to said encryption processing unit and by mixing processing

sequences of the original encryption processing units included in the original encryption processing sequence and said dummy encryption processing units **[abstract, pg. 11, lines 10-28]; “Another technique which could be used to improve resistance to attacks is to insert “dummy.” operation to confuse analysis of a power signature... The number of dummy look-ups performed can be chosen to optimize the time it takes to perform the DES operation and the benefit gained in DPA attack resistance”].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the encryption processing method of Kuo of the invention by including the step of Lin because it would perform the DES operation and the benefit gained in DPA attack resistance **[Lin, pg. 11, lines 18-19].**

Claims 9 and 22 are essentially the same as claim 19 except that they set forth the claimed invention as an apparatus / a computer program rather than a method and rejected under the same reasons as applied above.

As per claims 20, 10:

Claim 20

Kuo teaches an encryption processing method according to claim 19, wherein the encryption processing unit contained in said original encryption processing sequence is a single-DES encryption process, and said mixed encryption processing sequence setting step sets said dummy encryption processing unit as a single-DES encryption process **[pg. 56, section 3.5.1 Substitution, fig. 4; “The 256 bit data is**

broken down into 32 chunks, 8 bit each, and each of them is used as the address for S-box table lookup ... the block diagram for this module"; pg. 51; "The AES Rijndael algorithm was chosen in October 2000 and is expected to replace the DES and Triple DES"]. A motivation is the same as claim 19.

Claim 10 is essentially the same as claim 20 except that they set forth the claimed invention as an apparatus rather than a method and rejected under the same reasons as applied above.

Claims 6 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Henry Kuo et al.**, "Architectural Optimization for a 1.82 Gbits/sec VLSI Implementation of the AES Rijndael Algorithm", Springer-Verlag Berlin, LNCS 2162, pp. 51-64, 2001 in view of **Kocher et al.** (US 2001/0053220 A1).

As per claims 16, 6:

Claim 16

Kuo teaches An encryption processing method according wherein the original encryption processing sequence to be mixed is an encryption processing sequence including a triple-DES encryption process [pg. 51; "The AES Rijndael algorithm was chosen in October 2000 and is expected to replace the DES and Triple DES"].

Kuo does not explicitly teach a random-number generation process said encryption processing method further comprises the steps of forming a random-number generation process as a process including a conversion process by three single-DES

processes and setting the triple-DES encryption process as a random-number generation process in one of the groups of divisions.

However, Kocher teaches a random-number generation process and said encryption processing method further comprises the steps of forming a random-number generation process as a process including a conversion process by three single-DES processes and setting the triple-DES encryption process as a random-number generation process in one of the groups of divisions **[par. [0006]; “triple DES (a cipher constructed using three applications of Data Encryption Standard using different keys) can resist all feasible cryptanalytic attacks, provided that attackers only have access to the standard inputs to and outputs from the protocol”; par. [0008], lines 6-8; a key management devices introduce randomness]**.

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the encryption processing method of Kuo of the invention by including the step of Kocher because it would provide unpredictability into their internal state **[Kocher, par. [008]]**.

Claim 6 is essentially the same as claim 16 except that they set forth the claimed invention as an apparatus rather than a method and rejected under the same reasons as applied above.

Conclusion

The prior arts made of record and not relied upon are considered pertinent to applicant's disclosure.

US 2004/0047466 A1 to Feldman et al.

US 6,937,727 B2 to Yup et al.

US 7,043,016 B2 to Roelse, Petrus Lambertus Adrianus.


US 7,194,090 B2 to Muratani et al.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Canh Le whose telephone number is 571-270-1380. The examiner can normally be reached on Monday to Friday 7:30AM to 5:00PM other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Canh Le
August 10, 2007



CHRISTIAN LAFOLGIA
AU 2139